تشفير صورة Image Encoding
بواسطة خوارزمية RC6

ميمونة الحداد

Shrm_4fra@yahoo.com

Iraq-computer science

الخلاصة

يعتبر التشفير من المواضيع المهمة في هذا العصر بعد دخول التكنولوجيا إلى كافة نواحي الحياة العملية وكان لابد من وجود ما يحمي ممتلكات الأشخاص المتمثلة في الملفات الخاصة والعامة والتي نستخدمها بشكلها المفهوم مثل النصوص – الصور – الأصوات – المجلدات وغير ذلك من المعلومات.

وان الغرض من هذا البحث هو الحفاظ على امن وسرية المعلومات ضد عملية اختراق او كسر شفرة الصورة حيث انه يعتبر احد تطبيقات التشفير حيث يقوم بتشفير الصور التي نرغب بالحفاظ عليها من عبث المتطفلين ، وان الصورة المراد تشفيرها هي بهيئة 24bit BMP ويتناول هذا البحث طريقة توليد المفتاح ومن ثم استخدامه في تشفير الصورة المحددة ويتم فتح هذه الشفرة بنفس المفتاح ولقد تم تنفيذ هذه العملية بواسطة لغة البرمجة فيجيول بيسك دوت نت.

1- المقدمة:

ان التشفيرهو عملية الحفاظ على سرية المعلومات باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف الغير مفهومة.

لذلك تعبر كلمة " تشفير" عن تحويل أو " بعثرة" البيانات إلى هيئة غير قابلة للفهم لإرسالها عبر وسط ناقل معين إلى جهة محددة . بحيث لايمكن لأي جهة غير الجهة المقصودة تفسير هذة البيانات المبهمة واستخلاص البيانات المفهومة منها وهذة العملية هي أعلى درجة أمان ممكنة.

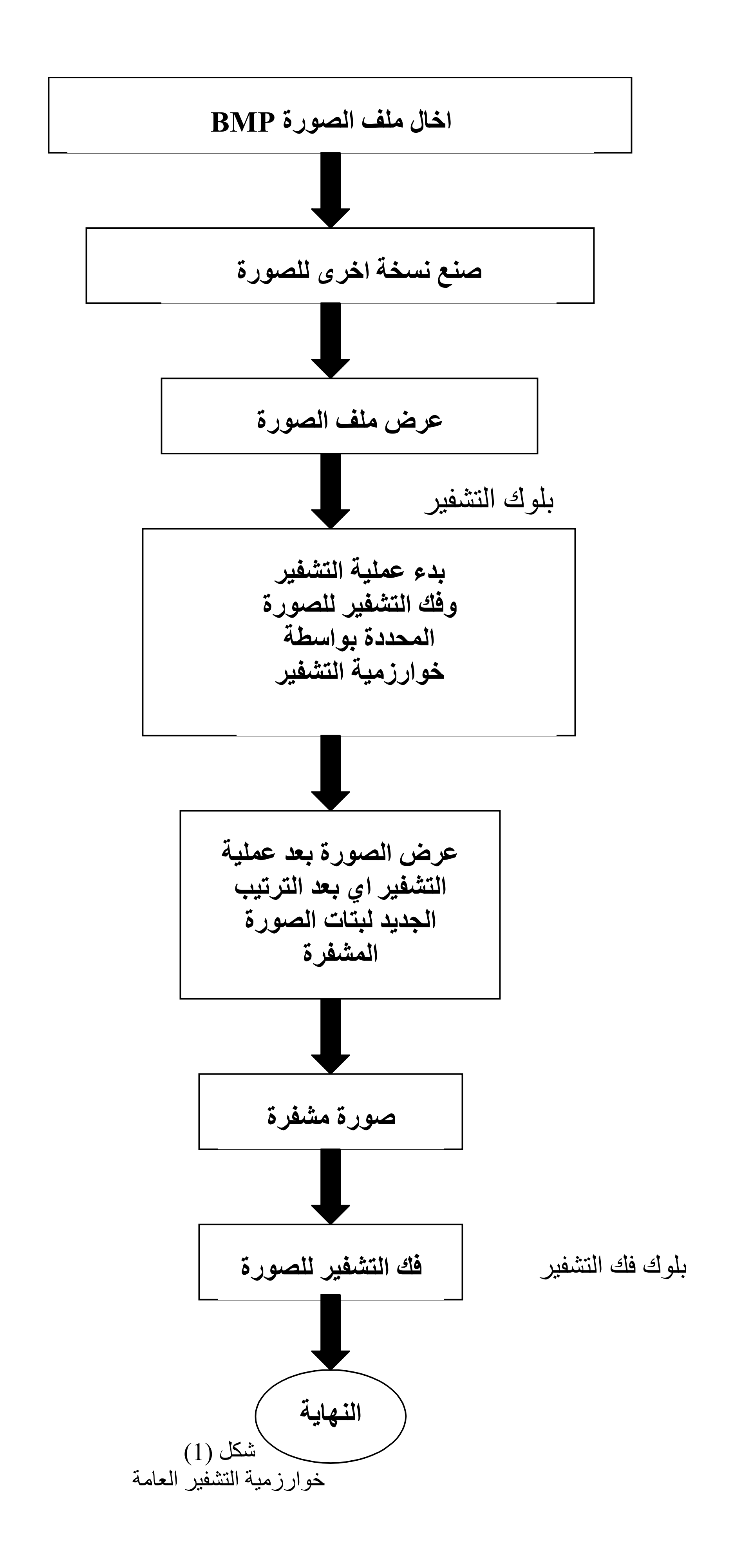
وفي بحثنا هذا قمنا بتطبيق مفهوم التشفير على الصور الرقمية ذات هيئة ملف(BMP 24 bit) والغرض من عملية تشفير الصور هو الحفاظ عليها من السرقة او العبث وخصوصاً اذا كانت صور خاصة او مهمة ولانرغب ان يراها احداً سوانا .

والصور هنا نتعامل معها على انها مجموعة من الارقام الثنائية حيث كل رقم في الصورة الرقمية يناظر مسافة صغيرة واحدة في الصور المرئية وهذه المسافة الصغيرة قد خصص لها عدد ثابت يسمى (Pixel) وهو يمثل اختصاراً لكلمة (Picture Element) وان حجم المساحة الفيزيائية بوحدة الصورة (Pixel) يسمى (Spatial Resolution) لوحدة الصورة.

4- خوارزمية التشفير العامة :

ان خوارزمية التشفيربصورة عامة للصور تشبه في مضمونها خوارزمية تشفير النص ولكنها تختلف في التعامل حيث ان ملف الصورة يعامل بصورة مختلفة عن ملف النص، حيث تركز عملية التشفير في الصورة على تشفيرالبتات لكل بكسلات الصورة وذلك يتم بواسطة مزج تلك البتات مع خوارزمية التشفير المحددة لينتج لدينا بكسلات مبعثرة وغير مفهومة وبالتالي تؤدي العمل المطلوب وهو الحصول على صورة مشفرة وغير واضحة المعاني وبهذا يتم الحفاظ على امن وسرية الصورة من العبث .

والمخطط التالي يوضح عملية التشفير للصورة بصيغة مفصلة وواضحة .

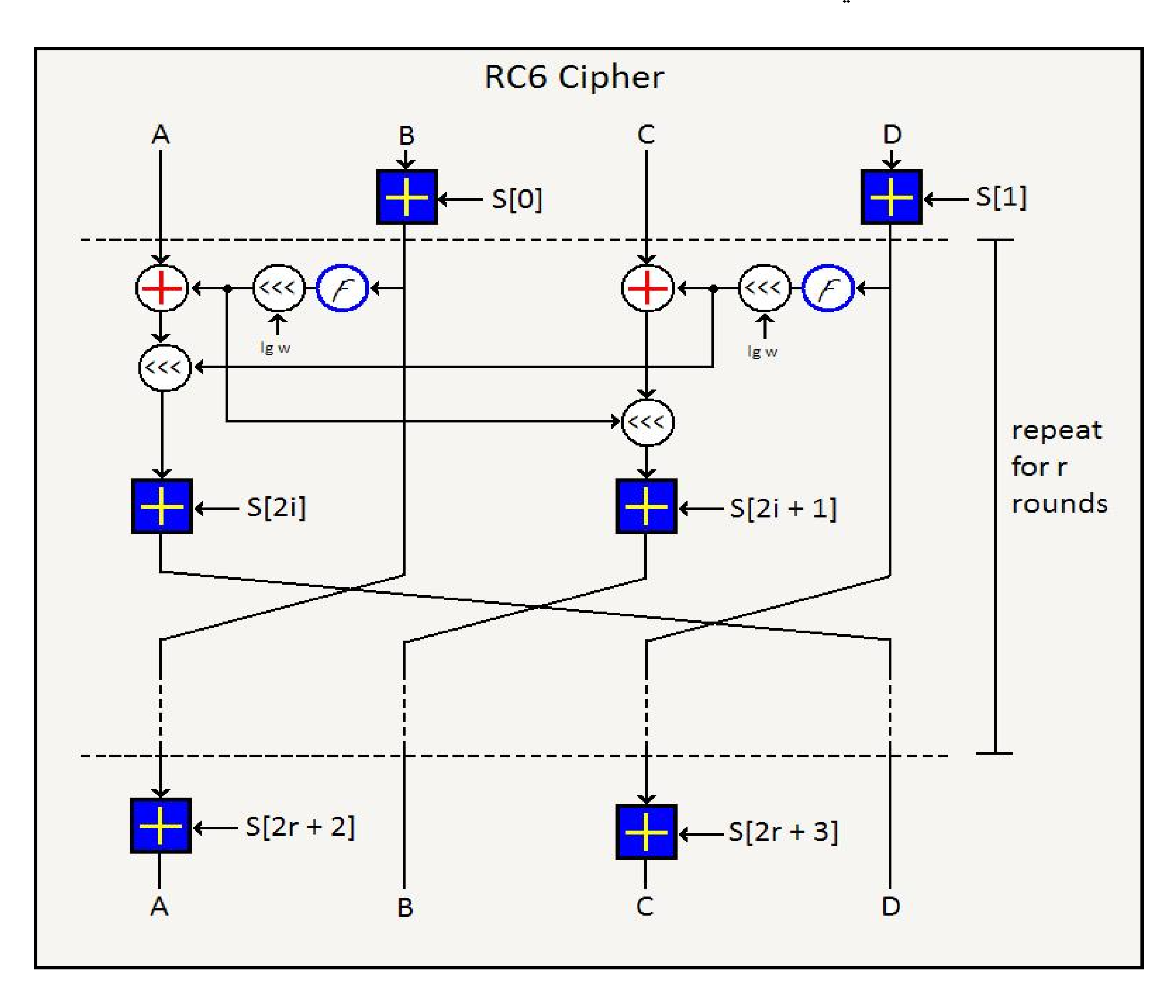


شكل (1)
خوارزمية التشفير العامة

ولقد تم استخدام خوارزمية التشفيرRC6 في هذا البحث لتشفير الصورة، وهذه الخوارزمية تعمل على بيانات الصورة المتمثلة بالبتات لكل بكسلات الصورة حيث تقوم هذه الخوارزمية بتقسيم مجموعة تلك البتات الى اربعة مجاميع هي A,B,C,D وبعد ذلك تقوم باجراء عمليات معقدة على تلك البتات وكما وضحنا سابقا .

5- خوارزمية RC6 :-

إن المخطط التالي يمثل خوارزمية التشفيرRC6 .



شكل (2)
خوارزمية RC6

وحسب مخطط RC6 فان عملية التشفير في هذه الخوارزمية تمر بعدة مراحل حيث يمكن ان نلخص عمل هذه الخوارزمية بالخطوات التالية :-

1- ادخال بلوك البيانات (حجمه 128 بت) .

- تقسيم البلوك الى اربعة اجزاء هي A,B,C,D وكل جزء يكون حجمه 32 بت.

-2 ادخال مفتاح التشفير ويكون حجمه 128 بت ايضاً ، ويبدأ دورته من S[0,..,2r+3].

-2-1 ناخذ الجزء الاول B ونجري عليه اول خطوات التشفير، حيث ناخذ الجزء B وندمجه مع المفتاح S[0] وحسب المعادلة الاتية : B=B+S[0]

-2-2 ان النتيجة التي تم الحصول عليها من الخطوة (1-2) تدخل الى دالة f ، وهذه الدالة تجري عمليات معقدة على تلك النتيجة حيث تقوم باضافة تصريح معين الى المفتاح او الكتلة او الاثنين معاً وذلك لزيادة شدة التعقيد ويمكن توضيح ذلك حسب المعادلات الاتية:-

Key =hash(password + salt)
For 1 to 65000 do
Key =hash(key +salt).

-2-3 ناخذ النتيجة من الخطوة (2-2) ثم نجري عليها عملية الازاحة لثلاثة مراتب حسب المعادلة الاتية :

. t = (B(2B+1)) <<< lgw

ملاحظة : نحول نتيجة هذه الخطوة (2-3) الى الجزء C وكما موضح في (شكل 2).

-2-4 بعد ذلك يتم اخذ الكتلة A ودمجها مع نتيجة الخطوة(2-3) بواسطة العملية xor ثم نضيف لها الناتج الذي تم الحصول عليه من الجزء D من خلال نفس العملية التي حصلت للجزء B في الخطوات (2-1...2-3) ثم تزحف التنيجة ثلاثة مراتب مرة اخرى.

-2-5 ناخذ نتيجة الخطوة (2-4) وندمجها مع المفتاح S[2i] بواسطة عملية xor وحسب المعادلة الاتية :

A= ((A^ t) <<< u) + S[2i]

-2-6 ان نتيجة الخطوات السابقة ادت الى تحول الجزء A الى D وحسب (شكل 2)
.

ملاحظة : كما لاحظنا في العملية التي جرت في الخطوات السابقة قد اختصرت بين الجزئين A وB فقط .

3- نجري نفس العمليات السابقة ولكن هذه المرة بين الجزئين D و C ، حيث ناخذ D ونجمعهُ مع المفتاح S[1] وتجري نفس العمليات من حيث التزحيف والدالة f ولكن مع اختلاف المعادلات ، وكما نلاحظ في المعادلات الاتية :

$u =((D (2D+1)) <<< lgw$
$C=((C \wedge u) <<< t) + S[2i+1]$

ملاحظة : ان هذه الخطوات تتكرر في كل دورة الى ان ينتهي عدد الدورات التي تمر بها الخوارزمية وهي 10 دورات .

4- ان النتائج النهائية التي نحصل عليها من هذه الخوارزمية هي كالتالي :

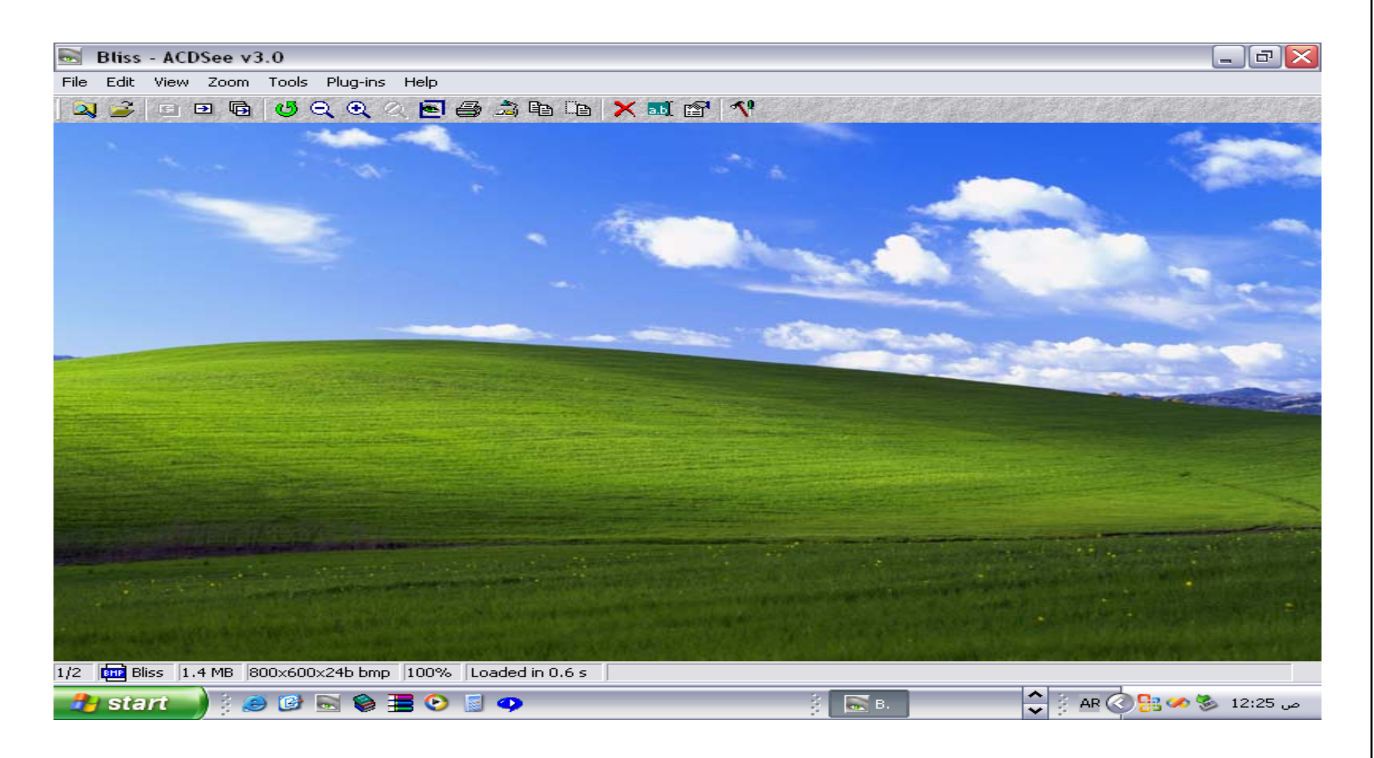
C ← D ، B ← C ، A ← B ، D ← A

ملاحظة : لكي نقوم بعملية فك الشفرة فاننا نتبع نفس الخطوات السابقة ولكن بصورة معاكسة (اي عكس عملية التشفير).

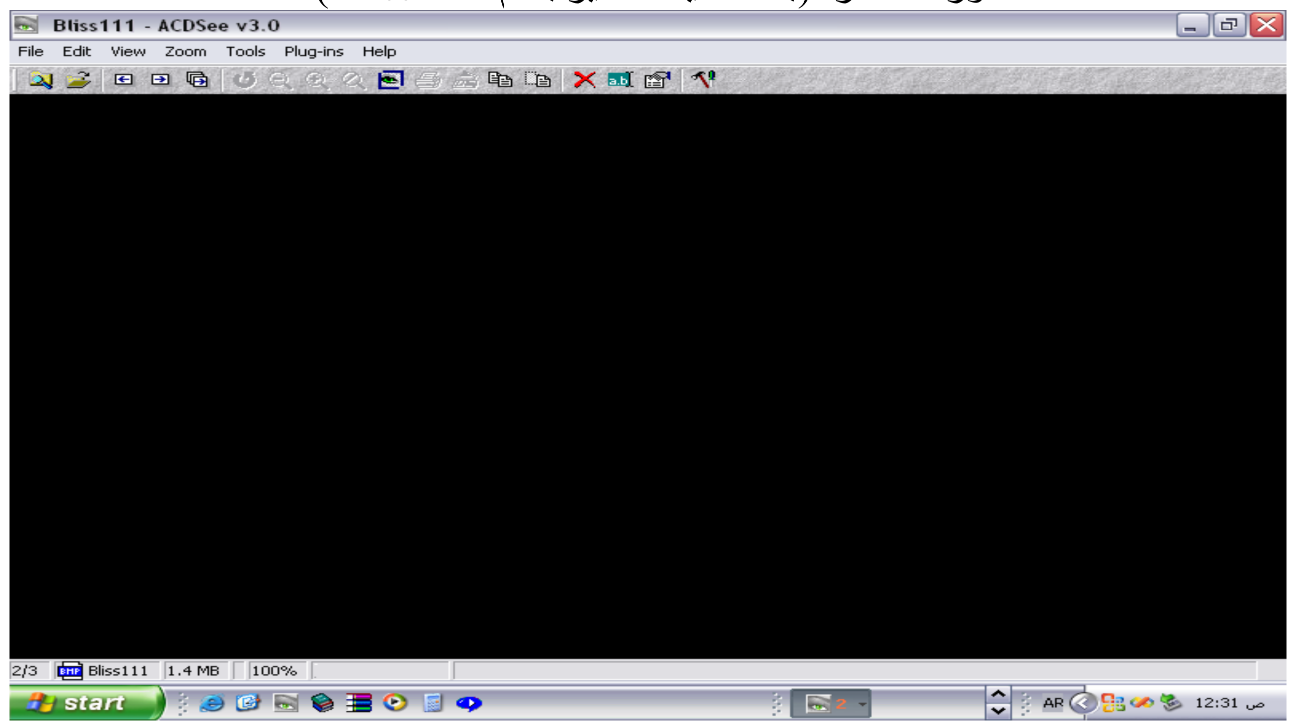
ولقد قمنا بكتابة برنامج يوضح عملية تشفير الصورة بشكل مفصل، حيث تبين واجهة تطبيق البرنامج المصممة بلغة فيجويل بيسك دوت نت كيف يتم تحديد اسم الصورة (BTISS) ومسارها من الحقل source file ومن ثم وضع المفتاح المحدد للتشفيرفي حقل key وهنا تم اختيار الكلمة computer كمفتاح ومن المفترض ان تظهر كلمة المفتاح بيصغة نجوم لحجبها عن الشخص الذي يحاول كسر خوارزمية التشفير ولكن للتوضيح تم اظهارها، واما الحقل destination فيتم فيه وضع اسم الصورة بعد تشفيرها بحيث تظهر الصورة المشفرة باسم جديد مثلاً (Btiss111)، ويجوز ان نبقي الصورة بنفس الاسم ولكن في هذه الحالة يجب تغير موقع الخزن لكي لايعترض الويندوز عليها .

واخيرًا لم يبقى لدينا سوى واجهة البرنامج لفك التشفير حيث تتم فيه نفس العملية السابقة ولكن يتم التعامل هنا مع اسم الصورة المشفرة (Btiss111)، حيث يُستخدم نفس المفتاح الذي تمت فيه عملية التشفير ويتم استدعاء الصورة في حقل source file ونعطيها اسم جديد ولنفرض مثلاً (Btiss222) في حقل destination ، وهذا يدل على ان الصورة يكون لها ثلاثة اسماء اسم قبل التشفير وبعد التشفيرواسم اخربعد فك التشفير.

الصورة الأصلية (قبل عملية التشفير باسم Btiss)



الصورة المشفرة (بعد عملية التشفير باسم Btiss111



المصادر

1- JONAS, GDMES and LVIZ, VELTIO.
"IMAGE PROSSING FOR COMPUTER GRAPHICS" , 1917 .

2- BIBER "CIPHER SYSTEM " , 1989 .

3- JEFF PROSISE " THE BMP FORMAT " , 1994 .

4- http://www.vc4arab.com